## IN THE DRAWINGS

Enclosed herewith are amended Figures 1D in which the proposed changes are made in an annotated marked-up drawing with a replacement sheet.

## IN THE SPECIFICATION

Paragraph 1051

Terminals 106A, 106B, 106C, 106D, 106E, 106F, 106G, 106H and 106I in the coverage area may be fixed (i.e., stationary) or mobile. As shown in FIG. 2, various terminals 106 are dispersed throughout the system. Each terminal 106 communicates with at least one and possibly more base stations 104 on the downlink and uplink at any given moment depending on, for example, whether soft handoff is employed or whether the terminal is designed and operated to (concurrently or sequentially) receive multiple transmissions from multiple base stations. Soft handoff in CDMA communications systems is well known in the art and is described in detail in U.S. Patent No. 5,101,501, entitled "Method and system for providing a Soft Handoff in a CDMA Cellular Telephone System", which is assigned to the assignee of the present invention.

Paragraph 1086

FIGS. 5A and 5B illustrate ~~FIG. 5B illustrates~~ the transmission and processing of keys, including RK, BAK and SK, according to an exemplary embodiment. As illustrated, at registration, the MS 300 receives the RK Information (RKI) and passes it to UIM 308, wherein the SUPU 316 computes RK using RKI and the A-key, and stores the RK in UIM memory storage SUMU 314. The MS 300 periodically receives the BAK Information (BAKI) that contains BAK encrypted using the RK value specific to UIM 308. The encrypted BAKI is decrypted by SUPU 316 to recover the BAK, which is stored in UIM memory storage SUMU 314. The MS 300 further periodically obtains SKI. In some exemplary embodiments, the MS 300 receives an

SKI_RANDOM that it combines with SKI_PREDICT to form SKI. The SUPU 316 computes SK from SKI and BAK. The SK is provided to ME 306 for decrypting broadcast content.

Paragraph 1098

FIG. 8B illustrates the subscription process in the system 500. The CS 502 further includes multiple encoders 504. Each of the encoders 504 receives one of the unique RKs and the BAK value generated in the CS 502. The output of each encoder 504 is a BAKI encoded specifically for a subscriber. The BAKI is received at the UIM of each MS, such as UIM$_1$ 512. Each UIM includes a SUPU and a SUMU, such as SUPU$_1$ 514 and SUMU$_1$ 510 of UIM$_1$ 512, and SUPU$_N$ 534 and SUMU$_N$ 530 of UIM$_N$ 532. The SUPU includes a decoder, such as decoder 516 or decoder 536 that recovers the BAK by application of the RK of the UIM. The process is repeated at each subscriber.

Paragraph 1099

FIG. 8D illustrates the processing of BC after registration and subscription. The CS 502 includes an encoder 560 that encodes the BC using the current SK to generate the EBC. The EBC is then transmitted to the subscribers. Each MS includes an encoder, such as encoder 544 or encoder 554, that extracts the BC from the EBC using the SK.

Paragraph 1118

FIG. 13 illustrates operation 900 of the CS. For each IP packet, the transmitter determines the BAK that will be used to derive SK, and determines the BAK_ID corresponding to the BAK at step 902. The BAK_ID may be any type of identifier that allows discrimination among multiple BAK values. The CS sends BAK and the BAK_ID to individual users by performing subscription at step 904. The users may perform subscription at various times before and during the subscription period. Steps 902 and 904 may occur before the subscription period starts. At step 906 the transmitter selects a RAND value and determines the corresponding RAND_ID. At step 908, the ~~The~~ CS may send RAND and RAND_ID to the MS individually or send RAND and RAND_ID to be broadcast on the broadcast channel. The value of RAND does not need to be secret, so it is not encrypted. If RAND and RAND_ID are broadcast, then there should not be much time between re-transmission so that an MS does not need to wait long before obtaining the RAND value. Broadcasting RAND and RAND_ID will use a large amount of bandwidth over time. However, if there are a large number of users tuned to the channel, then a large amount of bandwidth will be required to send RAND to each user individually. Consequently, RAND and RAND_ID should only be broadcast if there are a large number of users tuned to the channel. At step 910 the CS chooses a random value of SPI_RAND.

Paragraph 1119

Once the SPI_RAND, BAK_ID and RAND_ID are known, the transmitter combines them (e.g., concatenates RAND_ID and BAK_ID to the SPI_RAND) to form the SPI_SK at step 912. The CS uses a cryptographic function to combine SPI_RAND, BAK (identified by BAK_ID) and RAND (identified by RAND_ID) to form SK at 914. The CS then encrypts the broadcast message or portion of the message with SK at step 916, and transmits the encrypted message at step 918. Note that the encrypted broadcast message is part of an IP packet that includes the IP header and the ESP header. The ESP header includes the SPI_SK. At decision diamond 920, the CS decides whether to change SK. If the CS decides not to change SK, then the CS proceeds to step 916. If the CS decides to change SK, then the CS proceeds to decision diamond 922, where the CS decides whether to change RAND. If the CS decides not to change RAND, then the CS proceeds to step 910. If the CS decides to change RAND, then the CS proceeds to decision diamond 924, where the CS decides whether to change BAK. If the CS decides not to change BAK, then the CS proceeds to step 906. If the CS decides to change BAK, then the CS returns to step 902.

Paragraph 1126

Continuing with FIG. 7C, the method 440 initializes the timer t2 at step 442 to start the SK_REG time period T2. The CS generates SK_RAND and provides the value to transmit circuitry for transmission throughout the system at step 444. The timer t3 is initialized at step 446 to start the SK time period T3. The CS generates SK from SK_RAND, BAK, and TIME at step 448. The

CS then encrypts the BC using the current SK at step 450 ~~448~~. The encrypted product is the EBC, wherein the CS provides the EBC to transmit circuitry for transmission in the system. If the timer t2 has expired at decision diamond 452 ~~450~~, processing returns to step 442. While t2 is less than T2, if the timer t3 has expired at decision diamond 454 ~~452~~, processing returns to step 446, else processing returns to 450.

After paragraph 1127 and before paragraph 1128, insert the following:

FIG. 7E is a timing diagram of key update periods of a security option in a wireless communication system supporting broadcast transmissions.

Paragraph 1128

Key management and updates are illustrated in FIG. 8C, wherein the CS applies a function 508 to generate a value of SK_RAND, which is an interim value used by the CS and MS to calculate SK. Specifically, the function 508 applies the BAK value, the SK_RAND and a time factor. While the embodiment illustrated in FIG. 8C applies a timer to determine when to update the SK, alternate embodiments may use alternate measures to provide periodic updates, for example occurrence of an error or other event. The CS provides the SK_RAND value to each of the subscribers, wherein a function 518 or 538 resident in each UIM applies the same function as in function 508 of the CS. The function 518 operates on the SK_RAND, BAK and a timer value to generate a SK that is stored in a memory location in the ME, such as $MEM_1$ 542 of $ME_1$ 540 and $MEM_N$ 552 of $ME_N$ 550.